Remarks:

Reconsideration of the above referenced application in view of the enclosed amendment and remarks is requested. Claims 1–31 remain in the application. Claims 1, 8, 17, 24 and 27 are amended. Claim 32 is added to recite additional features of Applicant's invention, as described in the specification as originally filed.

ARGUMENT

35 U.S.C. § 112 Rejections:

Claims 24-26 are rejected under 35 U.S.C. §112 first paragraph, as failing to comply with the description requirement. This rejection is respectfully traversed and Claims 24-26 and their progeny are believed allowable based on the above amendments and the following discussion.

The Examiner asserts that the specification does not teach "when a message from an authorized party is not received as a BIOS; booting the system in a default state." One of ordinary skill in the art will understand the difference between default features and optional features. If there are no optional features selected, then the system will boot in a default mode. The alternative is that the system will not boot at all. Applicant's description in the specification does not teach or describe that the claimed invention fails to boot when no options are selected. This feature is inherent in the invention and will be understood by one of ordinary skill in the art. For instance, in the specification on pages 4 and 5, it is said "The capability of enabling optional system features is preferably secure, because the OEM may not want the system features to be enabled without authorization." As will be understood by one of ordinary skill in the art, if an optional feature is not authorized, the system will boot without optional features, e.g., in a default mode. Moreover, the Applicant describes on page 8, lines 10-13 of the specification that "If failure occurs (blocks 411, 412, and 413) during the decryption, authentication, or verification, process 40 is aborted, and the message is discarded (block 49)." At no time does the Application teach, suggest or imply that the system does not boot. It will be apparent to one of ordinary skill in the art that the system will boot without enabling the optional feature because the message

failed to be authenticated. Moreover, the specification describes, at least in conjunction with Fig. 2, that a message may be received while the system is already booted and that a reboot may be required. It will be obvious that if an authorization message is to be received while the system is running that it had to boot in some default state prior to receiving the message. In order to address all of the Examiner's concerns, Applicant amends Claim 24 to require that *when a message from an authorized party is not received at a BIOS: booting the system without optional features* in order to more closely match the language that is used in the specification. However, it is asserted that this amendment does not change the scope or meaning of the claim as originally presented. Therefore Claims 24-26 are believed allowable.

The Examiner rejects Claims 27-31 under 35 U.S.C. § 112 first paragraph, as failing to comply with the written description requirement. The Examiner also rejects Claims 27-31 under 35 U.S.C. § 112 second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. These rejections are respectfully traversed and Claims 27-31 and their progeny are believed allowable based on the above amendments and the foregoing and following discussion.

Regarding the rejection of Claims 27-31, the Examiner asserts that system resources are not defined as recited in the claims. Applicant respectfully, points the Examiner to at least page 3, lines 13-17 of the specification as originally filed. Applicant describes "*System resources 25 includes elements of system 10 that contribute to processing power, storage capacity, redundancy, and speed, e.g., memory, input/output devices, processors, redundant power supplies, and PCI (Peripheral Component Interconnect) bus.*" [emphasis added] Therefore, this rejection is improper and should be withdrawn. Applicant amends Claim 27 to remove the reference to "one or more of the resources", as suggested by the Examiner, to more clearly recite Applicant's invention.

Further, the Examiner asserts that capacity, redundancy and processor speed are not tangible resources. Applicant respectfully disagrees. A processor may be have multiple speed modes, selectable or authorized by an OEM. For instance a higher speed may require more power and a lower speed require less power. A user/owner may be required to pay more for a platform that operates at the faster speed, and this optional feature may be enabled or disabled by the OEM message, based on purchase price or licensing fee. Processor redundancy and capacity

are also not intangible optional features either, as suggested by the Examiner. If a second on-board processor, core, or thread is not authorized by the OEM, then the user cannot take advantage of processor redundancy. If enabled and authorized, redundant or parallel processing, for instance, may be implemented on the platform. Storage capacity is also not intangible. Optional features of system RAM, or cache or even flash memory may fall under the heading of "storage capacity." An OEM may base a purchase, lease or license fee on the quantity of various storage capacities. An entire bank of memory may be disabled if it is not explicitly authorized, which will then impact the effectiveness of the platform. Page 3 of the specification, beginning on line 18, also says: "Some of system resources 25 have system features that can be optionally selected or configured on an as-needed basis. The features generally include on/off status of the elements of system 10 and adjustable parameters of these elements, e.g., memory size, number of processors, number of PCI slots, PCI bus speed, number of redundant power supplies, and processor speed." Therefore, this rejection is improper and should be withdrawn.

35 U.S.C. § 102 Rejections:

Claims 1-4, 8-14, 17-20, 24 and 27-28 are rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Pat. No. 6,463,537 to Tello (hereinafter, "Tello"). This rejection is respectfully traversed and Claims 1-4, 8-14, 17-20, 24 and 27-28 and their progeny are believed allowable based on the above amendments and the foregoing and following discussion.

Claims 1, 8, 17, 24, and 27 have been amended to more clearly recite features of Applicant's invention. Claims 1, 8, 17 require that the authorized party is one of a manufacturer, OEM or lessor. This feature is not taught or suggested by Tello. Further, Claims 1, 17 and 27 require that when the message fails the authenticating, then discarding the message. This feature is not taught or suggested by Tello. Claims 8 and 24 require that the system is to boot without enabling the at least one optional feature when the secure message is not received from the authorized party. This feature is not taught or suggested by Tello. Therefore, 1-4, 8-14, 17-20, 24 and 27-28 are believed allowable.

Regarding Claims 2, 11-12 and 18, the Examiner asserts that Tello teaches *verifying an identifier in the message against a unique system identifier of the system.* Tello teaches identifying the purpose and type of the smartcard. Applicant maintains the argument that Tello does not teach or suggest a unique system identifier, and further, does not teach or suggest a message having an identifier to compare to the unique system identifier. Tello does not teach any message communication, but merely reading data in the smartcard and application of the data to authorize boot and data access. Specifically described at the cited reference, Tello teaches that the flash memory of the microprocessor has a secret identifier. However, Tello teaches that the identifier is 'the same for all motherboards." [Col. 9, lines 20-30] This argument was promoted because the Examiner misunderstands the implication of a single unique system identifier. Tello does not teach a system identifier. Tello teaches that each smartcard has a unique hash number or digital signature. Upon security setup, a complementary hash number is stored in the security engine microprocessor memory. Since Tello teaches a system that may be used by many users, each with their own smartcard, the security engine microprocessor may have many complementary hash codes stored for as many authorized smartcards. Further, a user may be authorized to use more than one system. Thus, the unique hash number is associated with the

smartcard and many systems may contain its complementary hash number to allow the user to boot each system. Thus, Tello teaches away from a "***unique system identifier of the system***" as recited in Claims 2, 11-12 and 18, and merely teaches a unique hash number associated with a smartcard. Moreover, with respect to claim 11, Tello does not teach a write-once non-volatile unit for storing a unique system identifier *accessible by the BIOS*. Thus, Claims 2, 11-12, 18 and their progeny are believed allowable.

Claims 3-4, 9-10, 13-14, 19-20 and 28 are believed allowable, at least, as being based on allowable base claims.

35 U.S.C. § 103 Rejections and § 103 (c) exclusion:

Claims 5 and 21 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Tello in view of U.S. Pat. No.6,581,159 to Nevis et al. (hereinafter, "Nevis et al.). This rejection is respectfully traversed and Claims 5 and 21 are believed allowable based on the foregoing and following discussion.

This discussion below was previously raised in the Applicant's Response to Office Action. The Examiner has improperly ignored this argument by citing MPEP § 706.02(l)(2). At no time does MPEP § 706.02(l)(2) require the Applicant to put the § 103 (c) discussion in a separate paper or page. The MPEP merely says that the applicant should put the argument in a separate paper or section so that the Examiner quickly notices it. Specifically, the MPEP says "The statement concerning common ownership **should** be clear and conspicuous (e.g., on a separate piece of paper or in a separately labeled section) in order to ensure that the examiner quickly notices the statement." [emphasis added] The Examiner should note that the use of the word "should" makes this statement optional, but preferred. Unless one of the words: *required, shall, must, mandatory*, etc. are used, then there is no actual requirement, but only a suggestion. Since in this case, the Examiner did notice the assertion of common ownership, as indicated by the Examiner's express rejection of it, no oversight occurred, and the argument should be deemed "clear and conspicuous." Instead, the Examiner has mandated a **suggested** procedure. This rejection is improper and the Examiner's refusal to apply the traversal is not only improper, but egregiously so. Therefore, Applicant respectfully requests that the Examiner **reissue a new office action** without citing the improper reference (Nevis et al.). Further, because this reference is improper, Claims 5 and 21 and their progeny are believed allowable and should be allowed to issue at the earliest possible time. The original argument is reiterated, below, for reference.

Without conceding the propriety of combining these references, Applicant respectfully submits that Nevis et al. cannot be used as a reference to render the present invention unpatentable. More specifically, Applicant respectfully points out that Nevis et al. is co-owned by the assignee of the present application. As articulated in 35 U.S.C. 103(c):

> "Subject matter developed by another person, which qualifies as prior art only under one or more of subsections (e), (f), and (g) of section 102 of this title, shall not preclude patentability under this section where the subject matter and the claimed

invention were, at the time the claimed invention was made, owned by the same person or subject to an obligation of assignment to the same person"

Since Nevis et al. does not qualify as a reference under 35 U.S.C. 102 (a), (b), (c) or (d), it may only be deemed prior art under 35 U.S. C. §102 (e), (f) or (g). As a result, pursuant to 35 U.S.C. §103(c), Applicant respectfully submits that Nevis et al. does not preclude patentability of the presently claimed invention since Nevis et al. and the presently claimed invention were, at the time the claimed invention was made, owned by the same person or subject to an obligation of assignment to the same person. More specifically, Nevis et al., which issued on June 17, 2003 as U.S. Patent No. 6,581,159, is assigned to Intel Corporation, the same entity to which the current application is assigned (assignment recorded on Oct. 1, 2001). As such, Applicant respectfully submits that Nevis et al. is an improper reference for use against the presently claimed invention and Applicant requests the Examiner to withdraw the rejection to Claims 5 and 21 under 35 U.S.C. §103.

35 U.S.C. § 103 Rejections:

Claims 6, 16 and 22 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Tello in view of U.S. Pat. No.6,704,789 to Ala-Laurila et al. (hereinafter, "Ala-Laurila et al.). This rejection is respectfully traversed and Claims 6, 16 and 22 are believed allowable based on the foregoing and following discussion.

Claims 6, 16 and 22 are believed allowable as being based on allowable base claims, as discussed above. Applicant further maintains that the combination of Tello with Ala-Laurila is improper because Tello teaches away from implementation of network transmission. Tello teaches that the smartcard is directly connected to the processor to determine authorization. This teaches away from communicating with the processor over a network transmission, as taught by Ala-Laurila.

Claims 7, 15 and 23 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Tello in view of U.S. Pub. No. 2001/0025312 to Obata (hereinafter, "Obata"). This rejection is respectfully traversed and Claims 5 and 21 are believed allowable based on the foregoing and following discussion.

Claims 7, 15 and 23 are believed allowable as being dependent on allowable base claims.

Claim 29 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Tello in view of U.S. Pat. No. 6,393,559 to Alexander (hereinafter, "Alexander"). This rejection is respectfully traversed and Claim 29 is believed allowable at least by being based on an allowable base claim. The Examiner has failed to make a prima facie case of anticipation for base Claim 27. The Examiner has not shown that each and every element of the base claim is taught by Tello. For instance, Claim 27 (and 29) require an authenticator to decrypt, authenticate and/or verify the secure message and to *discard the secure message if failure occurs during any one of decryption, authentication and verification.* Therefore, Claim 27 and its progeny, including Claim 29 are believed allowable. Further, Alexander teaches a system which may reboot a platform upon a failure to boot the first time, in order to correct the problem. It will be apparent to one of ordinary skill in the art that fixing a hardware problem is not the same as enabling the BIOS to control the at least one of the *optional* features. Alexander does not teach optional features, but teaches rebooting to correct a hardware error, for instance, to reinitialize corrupted memory and

change a flag from "resume from suspend" to "full reboot." (See Col. 3, lines 16-22) Moreover, Alexander does not teach or suggest a reboot according to the received secure message. Therefore, combining Tello and Alexander will not result in Applicant's claimed invention.

Claim 31 is rejected under 35 U.S.C. § 103 (a) as being unpatentable over Tello in view of U.S. Pat. Application No. 2003/0052906, now U.S. Pat. No. 6,633,309, to Lau et al. (hereinafter, "Lau et al."). This rejection is respectfully traversed and Claim 31 is believed allowable base on the foregoing and following discussion.

The Examiner asserts that Lau et al. teach *the secure message comprises executable code to be used as a Dynamically Loaded Library (DLL), and wherein the DLL is to be stored in non-volatile storage coupled to the BIOS, and wherein the DLL is to be loaded by the BIOS at run-time*. This assertion is flawed. Lau et al. teach putting plug-in modules in dynamic link libraries (DLL). Lau et al. do not teach or suggest that the DLLs are to be loaded by the BIOS at run-time. Lau et al. teach that

> "For a Microsoft Windows operating system environment, the plug-ins 16 are compiled as dynamic link libraries. At processing environment 10 run time, the shell 14 scans a predefined directory for plug-in programs. When present, a plug-in program name is added to a list which is displayed in a window or menu for user selection. When an operator selects to run a plug-in 16, the corresponding dynamic link library is loaded into memory and a processor begins executing instructions from one of a set of pre-defined entry points for the plug-in. To access a video sequence and video object segmentations, a plug-in uses a set of callback functions. A plug-in interfaces to the shell program 14 through a corresponding application program interface module 18." (Para. 37)

The Windows® run-time environment is discussed, but at no time do Lau et al. ever teach or suggest that the plug ins are coupled to or loaded by the BIOS. Therefore, the Examiner has failed to show a prima facie cases of obviousness and Claim 31 should be allowed to issue at the earliest possible time.

Claim 25 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Tello in view of U.S. Patent No. 6,584,561 to Merkin et al. (hereinafter "Merkin et al."). This rejection is respectfully traversed and Claims 5 and 21 are believed allowable based on the foregoing and following discussion.

Merkin et al. disclose a system and method for restricting a compact disk (CD) containing boot software to work only on computer systems for which the boot software has been authorized

to operate. Merkin et al. do not teach or suggest *splicing the contents of a message into the BIOS execution path*, as recited in the claims. Merkin et al. disclose that a computer system is checked for predetermined identification criteria to allow boot software from a CD to run on the computer system. Merkin et al. teach that a computer system may boot using the boot software on the CD. At no time do Merkin et al. disclose that a message is sent or that the contents of the message are used to alter a portion of the existing BIOS during boot. Instead, Merkin et al. teach a system where the system is booted using the entire boot software on the CD, not contents of a message. Merkin et al. teach replacing the existing boot software (BIOS) with the software on the CD to provide new boot software (Col. 2, lines 34-38). Applicant further points out that the limitations of Claim 25 are similar to claim 21. The Examiner conceded that Merkin et al. did not show the limitations of Claim 21 in the Office Action mailed on Aug. 5, 2005. Therefore, this rejection is improper and should be withdrawn. **Further, because the Examiner relies on an argument that Applicant has previously overcome, Applicant respectfully requests that the Examiner reissue a new office action without citing the improper reference.** All claims remaining in the application are now allowable.

CONCLUSION

In view of the foregoing, Claims 1 to 32 are all in condition for allowance. If the Examiner has any questions, the Examiner is invited to contact the undersigned at (703) 633-6845. Early issuance of Notice of Allowance is respectfully requested. Please charge any shortage of fees in connection with the filing of this paper, including extension of time fees, to Deposit Account 02-2666 and please credit any excess fees to such account.

Respectfully submitted,

Dated: 20 March 2006

/Joni D. Stutman-Horn/

Joni D. Stutman-Horn, Reg. No. 42,173
Patent Attorney
Intel Corporation
(703) 633-6845

c/o Blakely, Sokoloff, Taylor & Zafman, LLP
12400 Wilshire Blvd.
Seventh Floor
Los Angeles, CA 90025-1030

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☑ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.